Ventajas del hacking ético para las organizaciones

Placeres Salinas, Sandra Imelda;[1] Torres Mansur, Sandra Maribel[2]
& Barrera Espinosa, Azalea[3]

[1]Universidad Autónoma de Nuevo León, Facultad de Contaduría Pública y Administración, Monterrey, Nuevo León, México, sandra.placeressl@uanl.edu.mx, Av. Universidad S/N Col. Ciudad Universitaria, (+52) 81 8329 4000
[2]Universidad Autónoma de Nuevo León, Facultad de Contaduría Pública y Administración, Monterrey, Nuevo León, México, sandra.torresmn@uanl.edu.mx, Av. Universidad S/N Col. Ciudad Universitaria, (+52) 81 8329 4000
[3]Universidad Autónoma de Nuevo León, Facultad de Contaduría Pública y Administración, Monterrey, Nuevo León, México, azalea.barreraes@uanl.edu.mx , Av. Universidad S/N Col. Ciudad Universitaria, (+52) 81 8329 4000

Información del artículo arbitrado e indexado en Latindex:
Revisión por pares
Fecha de aceptación: Agosto de 2018
Fecha de publicación en línea: Diciembre de 2018

Resumen

Las organizaciones manejan información sumamente importante y crítica para su negocio, apoyándose de las tecnologías de información y sistemas para automatizar procesos y lograr ventaja competitiva; y así mantenerse en el mercado para subsistir; sin embargo, existen riesgos informáticos, por lo que pudieran tener comprometida su seguridad; dichos riesgos están a la orden del día y requieren identificar los que están asociados a su negocio para poder estar debidamente protegidos y evitar pérdidas tanto de información como económicas, ya que puede interrumpir su funcionamiento.
Se requiere la consultoría de un profesional de seguridad llamado "Hacker ético", el cuál detectará las vulnerabilidades y riesgos a los cuáles la empresa está expuesta y recomendar la solución más conveniente. El objetivo de esta investigación es que las empresas conozcan en que consiste y cuáles son las ventajas del hacking ético para identificar sus vulnerabilidades y riesgos, para enfrentarlos sin que estos les afecten de una manera importante.
.

Palabras claves: Análisis de riesgos, hacking ético, seguridad informática, delitos informáticos, buenas prácticas.

Abstract

Organizations today handle information that is critical for their business by using information technologies and systems to automate their processes and be able to get a competitive advantage; this way they would be able to survive in a difficult marketplace. However, there are IT related threats that may put their security at risk; those threats are consistent and need to be sighted, more specifically those that are related to their business in order to be properly protected and to avoid both informational and economical loss that would interrupt the business functionality.

Professional IT consulting service (also known as "ethic hacker") is needed. That service will be able to detect potential vulnerabilities and threats that the company is exposed to and, therefore, suggest possible and most convenient solutions. The objective in this paper is that businesses are aware of advantages of using ethical hacking to identify risk and vulnerabilities in order to face them before they affect them.

Key words: risk analysis, ethical hacking, informatic security, cybercrime, good practices.

1. INTRODUCCIÓN

En la actualidad, las empresas se apoyan completamente en las Tecnologías de información y comunicación (TIC) para soportar los procesos de negocio lograr una ventaja competitiva y por ende el éxito empresarial. La información sensible y crítica del negocio está expuesta o comprometida si no se tiene el cuidado de protegerla de intrusos o hackers que pudieran robar o manipular la información de la misma; por lo tanto, esta deberá de estar debidamente protegida y fuera del alcance de los mismos. Según Redman (2008), citado por Sánchez y Zúñiga (2011), si no contamos con información de calidad y confiable, esto nos podrá ocasionar problemas y costos para la organización.

Es recomendable que las empresas estén conscientes de que la información que manejan es muy importante y representa un activo intangible que también se deberá de proteger de posibles ataques y /o peligros. De ahí la importancia de que conozcan sus vulnerabilidades e implementen soluciones de seguridad, así como adopten buenas prácticas, que de acuerdo con Cárdenas, Becerra y Martínez (2013), "son un marco de referencias para asegurar que todas las organizaciones cubran todas sus bases de seguridad" esto ayudará a que los apoyen a minimizar los posibles riesgos detectados. Por lo que el objetivo de esta investigación es conocer, las ventajas del hacking ético y los riesgos informáticos a los que se enfrentan las organizaciones hoy en día, la importancia de conocer sus puntos vulnerables para posteriormente protegerse de una manera adecuada, tratando de reducir dichos riesgos.

2. MARCO TEÓRICO

Hoy día las empresas están conscientes de la gran importancia que tienen las TIC para el buen funcionamiento de la misma y de la manera en que esta genera valor a sus actividades empresariales. Es sin duda un componente vital para que las empresas puedan permanecer en la dura competencia a la que se tienen que enfrentar día a día; según Saavedra y Tapia (2013), es difícil en la actualidad visualizar una empresa exitosa sin el apoyo de las TIC. Son muchos los beneficios que las TIC aportan a los negocios, pero también trae consigo riesgos que pudieran impactar gravemente en la continuidad de las operaciones de los mismos.

Por ello se ven obligados a preocuparse por tener una seguridad informática lo suficientemente adecuada e invertir la cantidad óptima en Seguridad Informática, asegura Vera,G. y Vera, J. (2017), tomando como base modelos financieros o el análisis económico de costo-beneficio y evitando los riesgos que están latentes en la actualidad.

Según el pronóstico de Gartner (2017), se estima que las empresas aumenten su gasto en productos y servicios de seguridad en aproximadamente 93,000 millones de dólares en 2018. Esto debido al incremento de los ataques informáticos que están al alza; Aunque existe una gran preocupación al respecto, ya que de acuerdo al estudio realizado por McAfee llamado "Hackear la escasez de habilidades" trata de la escasez internacional de habilidades de ciberseguridad, donde respondieron a una encuesta países como: Reino Unido, Francia, Israel, Estados Unidos, Alemania, Japón, Australia y México y estos dos últimos países argumentaron que hay una gran cantidad de escasez de profesionales en seguridad cibernética, lo que implica que a las empresas se les dificultará y en el peor de los casos se incrementará el costo por los servicios de un hacker ético, ya que quizás tenga que solicitar los servicios a profesionales de otros países debido al déficit de profesionales en ese rubro.

Sin embargo, las empresas deberán de llevar a cabo un análisis costo- beneficio como propone Vera, G. y Vera, J. (2017), y ver todas las ventajas que se obtienen con los sistemas y el uso de las tecnologías que utilizan contra el costo asociado de los riesgos y vulnerabilidades que tendrían que pagar si estos se llegaran a presentar, afectando las operaciones normales del negocio. Una vez realizado ese análisis, se darían cuenta de la importancia de tener la seguridad informática para evitar problemas graves, y que estos pueden afectar al negocio reconociendo entonces que vale la pena invertir una buena parte de su presupuesto en seguridad para su negocio.

Las empresas saben que deben de extremar precauciones al respecto y adelantarse a los hechos, ya que bien vale la pena cuidar su información de los posibles ataques informáticos. Existen diferentes tipos de ataques que pueden afectar a las empresas hoy día y pudieran darse los siguientes: existen ataques activos y ataques pasivos, en el primer tipo de ataque se producen cambios en la información y en los recursos de los sistemas; en el segundo tipo registran el uso de los recursos o también pueden acceder a la información guardada o que es transmitida en los sistemas; otro riesgo no menos importante es el robo de información, donde se intercepta la información que es enviada entre las diferentes computadoras o dispositivos de la red de comunicaciones del negocio (Gómez, 2014).

El Instituto Nacional de Seguridad (INCIBE), ha publicado recientemente los 10 principales incidentes de ciberseguridad del año 2016 en todo el mundo ABC (2017):

1. Robo de 81 millones al Banco Central de Bangladés
2. Robo de 64 millones en bitcoins a Bitfinex
3. Publicación de los datos de 154 millones de votantes de E.E.U.U.
4. Publicación de información personal de 93 millones de mexicanos
5. Robo de millones de cuentas de yahoo
6. Robo de 500 millones de cuentas a yahoo (en 2014)
7. Robo de 400 millones de cuentas a Friend Finder Network
8. Ataque de denegación de servicio (DDoS) a Play Station y Twwiter entre otros
9. Fallo en la implementación de la pila TCP en sistemas Linux
10. Fallo en los procesadores Qualcomm

Se puede constatar que estos incidentes que se presentaron en el año 2016 afectaron de una forma importante a muchos negocios; así como pérdidas económicas, y daños en su reputación ya que sus clientes se dieron cuenta que no son de mucha confianza y la información de éstos no estaba debidamente protegida. Además, las actividades empresariales se vieron paralizadas y afectó la continuidad de las mismas, dañando tanto a la empresa como a sus clientes, proveedores y hasta ciudadanos.

Hacking ético

El hacker ético es: "un individuo capacitado para defender a las empresas de los ataques virtuales o crackers" Lara, F. (2009), también se le llama hacker de sombrero blanco quién tiene como su único y primordial objetivo " buscar vulnerabilidades en los sistemas de información o si no crear uno nuevo que permita actuar dentro de la legalidad y ética" Greenhill, K. (2010); no se le considera propiamente un delincuente en cuestión, se trata de que piense y actúe como delincuente con la única finalidad de que pueda defender a una organización y le ahorre muchos dolores de cabeza. "El objetivo del Hacker ético es ayudar a la organización a tomar medidas preventivas contra ataques maliciosos al atacar él mismo el sistema". Semana (2017).

El hacking ético según Secure IT, que es una empresa Española "es una práctica preventiva para evitar la actuación de los hackers y la sustracción de información confidencial o la destrucción de archivos importantes".

Existe una organización internacional llamada EC Countil , que tiene como función principal dar cursos y otorgar certificaciones en las áreas de seguridad de la información y comercio electrónico. Las personas que se hacen acreedoras a este tipo de certificación cuentan con habilidades que le permitirán detectar debilidades en los sistemas, utilizando algunas de las herramientas comúnmente conocidas por los hackers (Jauregui Lima , 2013). Básicamente se trata de burlar la seguridad de manera controlada de una empresa con la finalidad de implementar soluciones a dichas vulnerabilidades, implementando buenas prácticas, políticas y controles que ayuden a minimizar los riesgos existentes.

Seguridad informática

La seguridad informática se considera como "una disciplina del conocimiento, donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de una organización y así contar con estrategias que le permitan avanzar ante cualquier eventualidad." (Cano, 2004).

El objetivo primordial de la seguridad informática es el minimizar los riesgos en todos los recursos informáticos, garantizando la continuidad de las operaciones de la organización, mientras esta administra dichos riesgos a un costo aceptable (Voutssas, 2010). Para Ayala (2011), la seguridad informática en una organización es un proceso continuo, no un producto que debe comprarse o instalarse, se deben incluir actividades como la valoración de riesgos, prevención, detección y respuesta ante incidentes de seguridad.

Los elementos esenciales de la seguridad según comenta Malagón, (2010), son: la confidencialidad, que tiene que ver con ocultar la información o recursos; la autenticidad, es la identificación y garantía del origen de la información; otro elemento es la integridad que se refiere a los cambios no autorizados en los datos; y la disponibilidad que tiene que ver con la posibilidad de hacer uso de la información y recursos deseados en el momento en que se requiera.

Es muy importante que los negocios consideren a la seguridad informática como la mejor alternativa y la prevención como su mejor estrategia de seguridad. Entre los beneficios que otorga podemos mencionar que evita que los hackers maliciosos obtengan acceso a información restringida al contar con medidas preventivas adecuadas para evitar brechas de seguridad (Sánchez Carvajal, Manuel Henry; 2013).

Otros beneficios del hackeo ético es el contar con mayor conocimiento de los riegos y poder reducirlos, ahorro de tiempo y gastos al obtener los datos de los riesgos que se presentan para afrontarlos con tiempo o estar mejor preparados, mejora de la calidad de la empresas en el marco de seguridad, detección temprana de futuros fallos o detectar las brechas de seguridad (Malagón, 2010).

Según Voutssas (2010), las amenazas informáticas son eventos que pudieran ocasionar algún daño a los insumos informáticos de la organización, como: Malware o malicious software, pérdida, destrucción, alteración o sustracción de información por parte de personal de la organización, agregándole la consulta y divulgación de información de personas externas o grupos ajenos a la corporación con malas intenciones o con acceso no autorizado, por último la pérdida o destrucción de información debido a fallas de equipo o catástrofes naturales, ataques de negación de servicio o de intrusión a los sistemas de la organización por parte de ciber–criminales, los "phishers", especializados en robo de identidades personales y otros ataques del tipo de "ingeniería social"; Los "spammers" y otros mercadotecnistas irresponsables y egoístas quienes saturan y desperdician el ancho de banda de las organizaciones y el advenimiento de tecnologías avanzadas tales como el cómputo quantum.

Delitos informáticos

Los delitos informáticos son comportamientos ilícitos, según refiere Sánchez (2006), debido a su incorporación en todos los ámbitos de la sociedad, se generan ciertas acciones no adecuadas y en consecuencia por este tipo de situaciones no éticas los países las tienen tipificados en sus legislaciones y con sus sanciones correspondientes. Podemos resumir que son aquellas conductas en las que las Tecnologías de Información son el objetivo o medio de ejecución, aunque afecten a bienes jurídicos diversos (Villavivencio, 2014).

Algunos delitos informáticos que comúnmente se están dando hoy día en México según la Condusef, se reportó un incremento del 45 % en "robo de identidad en diversas modalidades como lo es fraude bancario, robo de identidad, estafa cibernética y clonación de tarjetas bancarias."

Buenas prácticas

Por lo descrito anteriomente, es necesario que toda organización que posea activos informáticos, debe contar con políticas de seguridad documentadas y procedimientos internos acerca de las estrategias y disposiciones que guíen los principales rubros y áreas relacionados con la seguridad de dichos bienes y que permitan su actualización y revisión por parte de un comité de seguridad interno (Voutssas, 2010).

Algunos de los principales objetivos de control y acciones que menciona Voutssas (2010), es crear políticas y procedimientos internos generales de seguridad informática, de acceso a instalaciones sensibles, de inventarios de bienes informáticos, de respaldo

de datos, de resguardo de información, para asignación de usuarios y lineamientos normativos de acceso, para la creación y mantenimiento de software.

Todos estos objetivos de control y acciones que mencionamos se logran implementando buenas prácticas y así contar con seguridad informática, algunas alternativas son: COBIT, ITIL, ISO 27001:2013. En relación al COBIT (Control Objectives for Information and related Technology), es un marco de referencia aceptado internacionalmente de buenas prácticas para el control de la información TI y los riesgos que conllevan.

El ITIL es una metodología basada en la calidad del servicio y el desarrollo eficaz y eficiente de los procesos, que cubren las actividades más importantes de las organizaciones en sus sistemas de información (Ramírez & Donoso, 2006). Esta metodología proporciona una guía de buenas prácticas de TI que son muy importantes para las empresas como son tareas, actividades, responsabilidades y procedimientos y una lista de verificación que cualquier tipo de empresa fácilmente puede implementar sin importa el tipo o giro del negocio.

Además de los anteriores, existe una norma de sistemas de gestión de seguridad de la información, denominada ISO 2700, la cual es reconocida a nivel internacional, esta maneja un marco de trabajo que identifica las mejores prácticas, permitiendo a las organizaciones identificar, analizar e implementar controles para la gestión de riesgos de seguridad de la información.

Otra opción es la auditoría de sistemas o auditoría informática, la cual ayuda a las empresas a comprobar si realmente funcionan los controles establecidos y las buenas prácticas anteriormente mencionadas que se han implementado para lograr la seguridad informática.Para Garzón, Ratkovich y Vergara ("s.f") la auditoría es la revisión y evaluación de los controles, sistemas y procedimientos de informática; está destinada a evaluar el cumplimiento de normativas, la gestión de los recursos, el funcionamiento y seguridad de los sistemas de información en las organizaciones (Gómez, Estrada, Bauta & García, 2012).

3. METODOLOGÍA

El enfoque metodológico aplicado para esta investigación fue conceptual documental; El diseño de la técnica de recolección de datos es analítico, ya que fue recabada de fuentes de información públicas y privadas, y de datos estadísticos de los últimos años y en artículos elaborados por expertos en el tema de hacking ético y seguridad informática.

La pregunta planteada para este estudio fue la siguiente:

¿Qué tan conveniente es el hacker ético en las organizaciones como una forma de lograr la seguridad informática?

A continuación se presenta el primer modelo para la identificación de los riesgos y sus acciones (figura 1), que servirá para determinar de manera formal y documentada los posibles riesgos a los cuáles la organización está expuesta de acuerdo al estudio preliminar que haya realizado el hacker ético.

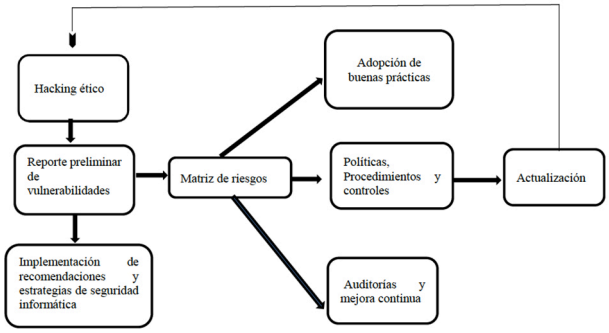
En el segundo modelo propuesto (figura 2), se muestra como lograr un nivel de seguridad mínimo aceptable en las oganizaciones teniendo en cuenta tareas importantes y buenas prácticas recomendadas.

Figura 1. Matriz de riesgos. (MR)

Riesgo	%Ocurrencia	Costo estimado asociado al riesgo	Acciones preventivas	Acciones durante la emergencia	Acciones correctivas	Políticas y procedimientos

Fuente: Elaboración propia.

Figura 2. Modelo del proceso de seguridad mínimo aceptable propuesto para las organizaciones.



Fuente: Elaboración propia.

4. RESULTADOS

Con base en la información recabada en esta investigación, el análisis de los datos y ante el incremento de los riesgos y delitos informáticos que se han estado presentando en las organizaciones a nivel mundial, se recomienda que para lograr una seguridad informática efectiva, se contrate los servicios de un hacker ético para que realice un escaneo y un estudio de vulnerabilidad informática y se detecten los riesgos latentes que pueda tener la organización. Teniendo esta información podemos utilizar la matriz de riesgos (MR) aquí propuesta, para analizarlos y documentarlos e ir identificando las diferentes acciones y soluciones que tendremos que implementar para lograr la seguridad informática en la organización.

La MR servirá para identificar de manera formal y documentada, los posibles riesgos a los cuáles la organización está expuesta de acuerdo al estudio preliminar del hacker ético, y para cada uno de ellos conocer su porcentaje de ocurrencia, el costo asociado al riesgo, que nos permitirá tener un aproximado de cuanto nos costaría y conocer las acciones que deberemos de realizar o llevar a cabo en diferentes etapas del mismo, ya sea en una primera etapa como prevención, en una segunda etapa acerca de cómo poder enfrentarlos en el momento justo en que el riesgo se presente y en una tercera etapa las acciones que se tendrán que realizar y son necesarias para poder remediar los inconvenientes y daños que nos haya ocasionado.

Por último diseñar políticas y procedimientos para cada uno de los riesgos identificados, con la finalidad de reducir el porcentaje de ocurrencia de cada uno de éstos. Tal vez no podremos eliminar-

los todos, pero si disminuir el porcentaje de que ocurran y controlarlos de forma interna: educando y enseñándoles a los empleados del negocio como podemos prevenir los riesgos.

Esta Matriz nos ayudará a lograr identificar los riesgos y prevenir algún ataque, y si se llegara a presentar, saber cómo enfrentarlos y salir menos dañados, todo esto gracias al estudio preliminar que el Profesional de TI en este caso el hacker ético hizo y de esta forma podremos tener seguridad informática en las organizaciones.

El modelo del proceso de seguridad mínimo aceptable (aquí propuesto) para las organizaciones, nos servirá como guía para no perder el camino a seguir en cuanto a las actividades que se tendrán que llevar a cabo para lograr y mantener la seguridad informática.

Es indispensable en todo momento apoyarse con profesionales de TI para que nos recomienden la mejor solución y estrategia. Además, deberá de adoptarse buenas prácticas reconocidas a nivel mundial como: COBIT, ITIL e ISO 27001:2013

5. CONCLUSIONES

Todas las organizaciones ya sean públicas o privadas, sin importar el giro del negocio o actividad a la que se dediquen, primeramente deberán de estar convencidos de que tienen que invertir en Seguridad Informática, y que no es un dinero mal invertido ya que su información es crítica y muy valiosa para poder funcionar de una manera óptima y tomar buenas decisiones, y si se presenta un riesgo o un ataque informático podrán verse afectados sus datos e inclusive perderlos por no haber tenido la seguridad necesaria para poder evitarlos. Deberán de reconocer los beneficios y el valor que le generan las TIC, para poder apreciar que deben de cuidar celosamente a su empresa.

Las empresas deberán de contratar los servicios profesionales de un Hacker ético. Este profesional ayudará a identificar riesgos y vulnerabilidades a las que están expuestas las organizaciones ante el aumento de delitos informáticos hoy día. Deberán de implementar las estrategias de seguridad y buenas prácticas, marcos de referencia que se les recomienden para evitar salir afectados por cualquier riesgo o inseguridad detectada.

Además, las organizaciones deberán de actualizar de forma constante los objetivos de control, las políticas y procedimientos, así como los riesgos identificados en la matriz de riesgos fig.1 cada vez que se realice un estudio de vulnerabilidad y riesgos detectados por un hacker ético, implementando el software o tecnologías adecuadas para lograr la seguridad informática.

Se recomienda que si en la empresa existe un departamento o área de TI, se capacite y prepare debidamente mediante alguna certificación a alguno de los integrantes de esa área, para que pueda ser en el futuro profesional de TI y sea el hacker ético (sombrero blanco) de la organización.

Un aspecto muy importante y que ayudará a reducir en parte los ataques o riesgos es capacitar a los usuarios o empleados de las empresas con buenas prácticas de seguridad y de esta forma no participen en el aumento de estos.

Podemos afirmar que “La prevención es la mejor estrategia y arma de seguridad en las organizaciones.” Se recomienda no escatimar nunca en la seguridad, ya que es una buena inversión, que nos ayudará a mantener y proteger a las organizaciones a salvo de los riesgos y ataques que comúnmente se enfrentan hoy día ,más vale invertir que tener que lamentar un desastre o que las organizaciones pierdan su valiosa información.

REFERENCIAS

Ayala, G., Gómez Julian (2011) Guía de buenas prácticas de seguridad de la información para micros pequeñas y medianas. Universidad Tecnológica de Pereira. ISSN 0122-1701. http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2514/0058A973_anexo.pdf?sequence=2

Cano, J. J. (2004). Inseguridad Informática: un concepto dual en seguridad informática. (Spanish). *Revista de Ingeniería*, (19), 40-44.

Cardenas, S.,Becerra, A.& Martínez, A. (2013). Gestión de la seguridad de la información: un marco de trabajo. Recolectado de http://congreso.investiga.fca.unam.mx/docs/xviii/docs/2.04.pdf, 2013 ANFECA

Castrillo, J.(2018).Cuando la identidad física y la identidad móvil coexisten, hay más beneficios en seguridad. *Revista mas seguridad.* Recolectado http://www.revistamasseguridad.com.mx/2018/01/24/cuando-la-identidad-fisica-la-identidad-movil-coexisten-mas-beneficios-seguridad/

Castro Rojas, J. E., Farigua Gutiérrez, J. A. y Suárez Cortés, L. E. (2016). Guía de auditoría para evaluar el aseguramiento de la disponibilidad e integridad de la información en el sistema de contratación de la Secretaria Distrital de Integración Social, basada en la norma ISO 27001:2013. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Auditoría de Sistemas de Información. Bogotá, Colombia

Cifuentes, C. (2017). Los diez mayores ataques informáticos de 2016. *ED Economía digital*. Sección Tecnologías y Tendencias. Recolectado de 5 abril 2018. https://www.economiadigital.es/tecnologia-y-tendencias/los-diez-mayores-ataques-informaticos-de-2016_188964_102.html

Computer World México (2017) México.Recolectado de http://computerworldmexico.com.mx/la-inversion-en-seguridad-aumentara-7-en-2017-estima-gartner/

Felipe Villavicencio, T. F. (2014) Delitos Informáticos.IUS ET VE RITASNo.49,285-304.http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Garzón, Ratkovich, Vergara ("sin fecha"). Metodología de análisis de vulnerabilidades para empresas de media y pequeña escala. Recolectado de: http://hermes.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

Gil Vera,V., & Gil Vera, J (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica, 22*(2), 193-197.

Gómez A. V (2014) Tipos de ataques y de intrusos en las redes informáticas. Recolectado de http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf.

Gómez Baryolo, O., Estrada Sentí, V., Bauta Camejo, R. R., & García Rodríguez, I. (2012). Modelo de gestión de log para la auditoría de información de apoyo a la toma de decisiones en las organizaciones. (Spanish). *Acimed*, *24*(2), 187-200.

Greenhill, K. (2010). Transformando la biblioteca pública: de conservadores de ediciones impresas a creadores de contenido digital.

ISO 27001 Para la mejora del rendimiento en seguridad de la información. http://www.lrqa.es/Images/28141-datasheet-isoiec-27001-de-sistemas-de-gestin-de-se.pdf

Jauregui, L. ¿Qué Comprende Ethical Hacking?. RITS. 2013, n.8 [citado 2018-03-20], pp. 9-10 . Disponible en: <http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442013000100005&lng=es&nrm=iso>. ISSN 1997-4044.

Lara, F. (2009). Escuela para hackers. (Spanish). *Contenido*, (550), 40-45.

Mcafee (s.f) Hacking the Skills Shortage. Recolectado de https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

Malagón, C. (2010). Nerbrija Universidad de Madrid. Obtenido de Nerbrija Universidad de Madrid: http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_0.pdf

Montaño O. V. La gestión en la seguridad de la información según Cobit, Itil e Iso 27000

Ramírez, B.P. Y Donoso, J. F. (2006) http://repositorio.uchile.cl/handle/2250/108405

Revista Pensamiento Americano ISSN: 2027-2448 Vol 2 No. 6. Enero – Junio 2011 (Págs 21-23)

Sanchez, G.E y Zuñiga S. L (2011).Revista Nacional de administración. Volumen 2 (2) 145-154.

Sanchez, C. y Henry, M. Ethical Hacking: La Importancia de una intrusión controlada. RITS [online]. 2013, n.8 [citado 2018-03-21], pp. 11-13 . Disponible en: <http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442013000100006&lng=es&nrm=iso>. ISSN 1997-4044.

Sánchez Curbelo, B. V. (2006). Las nuevas tecnologías y los delitos informáticos. (Spanish). *Tono: Revista Técnica De La Empresa De Telecomunicaciones De Cuba, S.A,* (3), 14-19.

Saavedra García, M.,& Tapia Sánchez, B. (2013). El uso de las tecnologías de información y comunicación TIC en las micro, pequeñas y medianas empresas (MIPyME) industriales mexicanas. Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento, 10(1), 85-104.

Secure &IT (2015). Los beneficios del hacking ético para las empresas. Recolectado https://www.secureit.es/los-beneficios-del-hacking-etico-para-las-empresas/#

Semana (2017). Como ser un hacker profesional Recolectado http://www.semana.com/educacion/articulo/hacker-como-ser-un-hacker-profesional/525664

Valladolid (2017). Diez principales incidentes en ciberseguridad de 2016. Recolectado http://www.abc.es/espana/castilla-leon/abci-diez-principales-incidentes-ciberseguridad-2016-201702131420_noticia.html

Voutssas M., Juan. (2010). Preservación documental digital y seguridad informática. Investigación bibliotecológica, 24(50), 127-155. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008